UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/810,927	03/25/2004	Carl E. Banzhof	4059-01200	1914

30652 7590 12/15/2006

CONLEY ROSE, P.C.
5700 GRANITE PARKWAY, SUITE 330
PLANO, TX 75024

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 12/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/810,927	**Applicant(s)** BANZHOF ET AL.	
	Examiner Carl Colin	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *3/25/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Pursuant to USC 131, claims 1-31 are presented for examination.

Claim Objections

2. Claims 22-29 are objected for the following informalities: "the apparatus of" should be replaced with --the computer network of-- or appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3.1 **Claims 1-3** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Publication 2003/0163728 to **Shaw**.

As per claim 1, **Shaw** discloses a method for protecting a computer network from vulnerabilities, comprising: *quarantining* (detaining in a virtual lobby) *a computer system* (client) *seeking to connect to said computer network until said quarantined computer system is remediated* (see page 3, paragraph 34); *and upon completing remediation of said quarantined computer system, connecting said remediated computer system to said computer network* (see page 3, paragraph 34).

As per claim 2, **Shaw** discloses the detaining is performed on-connect that meets the recitation of *wherein said quarantine of said computer system is self-initiated* (see page 3, par. 34).

As per claim 3, **Shaw** discloses scanning, security mechanisms and configurations (*remediation)* are performed by a network security authority or delivery assistant that meets the recitation of *wherein said remediation of said computer system is performed by said computer network* (see pages 3-4, par. 38 and par. 42).

3.2 **Claims 7-8** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 7,089,589 to **Chefalas et al.**

As per claim 7, **Chefalas et al** discloses *for a computer network comprised of a plurality of computer systems and a client remediation server coupled to each one of said plurality of computer systems, said client remediation server remediating said computer network by resolving vulnerabilities in said plurality of computer systems, a method for protecting said remediated computer network from unresolved vulnerabilities, comprising:*

if one of said computer systems (offending system) *of said remediated computer network is disconnected from said remediated computer network, upon a subsequent re-connection of said computer system to said remediated computer network, temporarily limiting exchanges between said remediated computer network and said computer systems* (see column 9, lines 29-44). **Chefalas et al** discloses above verifying that the offending system is disinfected before allowing reconnection to the network that meets the recitation of *temporarily limiting exchanges between said remediated computer network and said computer system.* **Chefalas et al** further discloses disabling the user account (see column 5, lines 52-53) that also meets the recitation of temporarily limiting exchanges between the computer system and the network.

As per claim 8, **Chefalas et al** discloses limiting exchanges between the offending system and other devices until the offending system has been disinfected that meets the recitation of *wherein exchanges between said computer system and said remediated computer network are limited until said computer system has been checked, by said client remediation server, for pending remediations* (see column 9, lines 35-44).

3.3 **Claims 21-26 and 29** are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent Publication 2005/0188419 to **Dadhia et al.**

As per claim 21, **Dadhia et al** discloses a *remediated computer network comprising: a computer system* (see figure 1 and page 2, paragraph 18)*; and a client remediation server coupled to said computer system,*(see par. 18, last sentence) *said client remediation server* *configured to periodically resolve vulnerabilities in said computer system* (see page 1, paragraph 5); **Dadhia et al** discloses the computer system may perform a rule where the instance of the application has access only to only resources that will allow it to update (resolve vulnerabilities) (see par. 25) and further discloses restricting the instance access until a patch to a vulnerability that has been exploited by a worm has been installed (see paragraph 12) that meets the recitation of *wherein said computer system includes a firewall for periodically isolating said computer system, from said remediated computer network, until said client remediation server resolves vulnerabilities of said computer system.*

As per claim 22, **Dadhia et al** discloses dropping network communication so that the vulnerability of the instance is not exploited that meets the recitation of disconnects from the network (see page 1, paragraph 12) and discloses the dynamic protection system establishes limitations through actions of rules when an instance of an application first executing (see page 2, paragraph 14) or first attempts to access a network resource after startup (see page 4, claim 2), that meets the recitation of *wherein said computer system is configured to raise said firewall to isolate said computer system from said remediated computer network whenever said computer system disconnects from and subsequently reconnects to said computer network;* the filter rules are explained in more details in paragraph 19.

As per claim 23, **Dadhia et al** discloses *wherein said computer system is configured to raise said firewall upon each power-up thereof* (see page 4, claim 2).

As per claim 24-26 and 29, **Dadhia et al** discloses the claimed network of claim 22 and further discloses the *computer system is configured to raise said firewall upon initiating registration with a LAN* (see paragraph 18). **Dadhia et al** discloses that the invention may be implemented with the Internet, LAN, WAN, network handheld or laptop devices *(wireless devices*) attached to the network, (see paragraphs 20-21) that meets the recitation of *wherein said remediated computer network is a local area network (LAN), a wide area network (WAN), a wireless local area network (WLAN), the Internet and said computer system is configured to raise said firewall upon initiating registration with said LAN, WAN, WLAN and the Internet.*

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.1 **Claims 4-6 and 14** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication 2003/0163728 to **Shaw**.

As per claim 4, **Shaw** substantially discloses the claimed method of claim 1. **Shaw** discloses the client has a software firewall 712 (see page 4, par. 38). Although **Shaw** does not explicitly disclose that the computer system (client) raises the firewall 712 *for blocking traffic between said computer system and said computer network.* Examiner takes official notice that it is notoriously well known in the art that a firewall is designed for blocking traffic between a computer system and a network and also for allowing specific traffic to go through according to a design choice. **Shaw** discloses that the virtual lobby between the client and the computer network contains a firewall that protects the lobby against the outside world and another firewall protects the network from clients. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to raise the firewall of the client for blocking traffic between the client and the network to protect itself against the network until ensuring that the network is trusted.

As per claim 5, **Shaw** discloses the claimed method of claim 4 and further discloses a software component 404 for providing security mechanism to the client so that the client complies with the security requirements (see page 2, par. 24), it is apparent to one of ordinary skill in the art that to provide the security requirements, the client firewall has to permit the software there through; therefore, the disclosure of **Shaw** meets the recitation of *wherein said firewall permits a flow of vulnerability resolution information therethrough.*

As per claim 6, **Shaw** discloses the claimed method of claim 5 and further discloses allowing scanning and delivery from the network to the client that meets the recitation of *lowering said firewall after said computer system has been remediated using said vulnerability resolution information* (see page 2, par. 24). **Shaw** also discloses after the client is remediated the virtual lobby firewall allows the client to have access to the network (see page 2, paragraph 26). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the virtual lobby firewall features into the client firewall so that the client could have control of when to allow or block traffic as suggested by **Shaw** (see paragraph 19).

As per claim 14, **Shaw** substantially discloses *a method for protecting a computer network from nefarious software associated with a computer system being connected to said computer network, comprising: upon initiating a connection between said computer system and said computer network, quarantining* (detaining in a virtual lobby) *said computer system from said computer network* (see page 3, paragraph 34); *performing a scan on said computer system* (see page 3, paragraph 34); **Shaw** discloses a virus scanner configured to check for particular virus and ensuring that the client has the latest virus patches (see paragraphs 18 and 38) before allowing client access to the network "to avoid risks like spreading viruses" (par. 17, last sentence) that meets the recitation of *lifting said quarantine of said computer system upon completing the removal of any nefarious software detected by said scan.* Although Shaw is silent about "removal of virus", it is apparent to one of ordinary skill in the art that an antivirus scanner with the latest patches would have the tool necessary the remove the virus when found. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the feature of removing the virus as part of the scanning process of **Shaw** "to avoid risks like spreading viruses" as suggesting by ***Shaw*** (see page 1, par. 17).

4.2 **Claims 9-13** are rejected under 35 U.S.C. 103(a) as being unpatentable by US Patent 7,089,589 to **Chefalas et al** in view of US Patent 5,987,611 to **Freund** *(Applicant's disclosure).*

As per claim 9, **Chefalas et al** substantially discloses the claimed method of claim 7. **Chefalas et al** suggests the server "raising a firewall upon reconnection" by blocking reconnection request which is a filtering process performed by firewall as it is known in the art, but does not explicitly disclose the computer system raising a firewall upon reconnecting. **Freund** in an analogous art discloses a client-based filter application *(firewall)* for monitoring whether client process has access to the Internet otherwise the remediation for any violated rule is performed (see column 4, lines 29-33 and lines 54-63); and further discloses limiting the user access to the network in case of any problems including malfunction, tampering,with remediating the network (see column 22, lines 30-41); **Freund** discloses in a preferred embodiment all the filtering process may be performed by the client-based filter application *(firewall)* (see column 4, lines 29-33). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have the offending computer system raised a firewall upon reconnecting to the network. One of ordinary skill in the art would have recognized some of advantages suggested by **Freund** for having the user firewall performing some of the filtering work; the advantages of doing so would reduce the workload of the server and would avoid a centralized filtering mechanism misinterpreting the rules to apply to data packets as suggested by **Freund** (see column 2, lines 38-46 and 59-63).

As per claim 10, the references as combined above disclose *filtering out non-remediation-related traffic between said computer system and said remediated computer network* (see **Freund,** column 4, lines 29-33).

As per claim 11, the references as combined above disclose the claimed method of claim 10. **Chefalas et al** further discloses the server grants access to the computer system and the computer system resumes normal operation upon verification that the computer system is disinfected that meets the recitation of *removing said limitations on exchanges between said computer system and said remediated computer network upon said client remediation server executing said pending remediations for said computer system* (see **Chefalas et al**, column 8, lines 58-64 and column 10, lines 29-33).

As per claim 12, the references as combined above disclose the claimed method of claim 11. **Chefalas et al** further discloses the server grants access to the computer system and the computer system resumes normal operation that meets the recitation of *wherein removing said limitations on exchanges between said computer system and said remediated computer network further comprises said computer system lowering said firewall* (see column 8, lines 58-64). **Freund** discloses the user will not gain access to the rest of the Internet until the user downloads the client Monitor component that also meets the recitation of that meets the recitation of *wherein removing said limitations on exchanges between said computer system and said remediated computer network further comprises said computer system lowering said firewall* (see column 22, lines 38-40).

As per claim 13, the references as combined above disclose the claimed method of claim 11. **Chefalas et al** further discloses the server grants access to the computer system and the computer system resumes normal operation that meets the recitation of *permitting non-remediation-related traffic to pass between said computer system and said remediated computer network without filtering* (see column 8, lines 58-64). **Freund** discloses the user will not gain access to the rest of the Internet until the user downloads the client Monitor component that also meets the recitation of that meets the recitation of *permitting non-remediation-related traffic to pass between said computer system and said remediated computer network without filtering* (see column 22, lines 38-40).

4.3 **Claims 15-20** are rejected under 35 U.S.C. 103(a) as being unpatentable by US Patent Publication 2003/0163728 to **Shaw** in view of US Patent 5,987,611 to **Freund** *(Applicant's disclosure).*

As per claim 15, **Shaw** substantially discloses the claimed method of claim 14. **Shaw** discloses the client has a software firewall 712 (see page 4, par. 38) and also discloses *wherein said computer system is quarantined from said computer network by a firewall residing on a* network security authority. **Shaw** does not explicitly disclose that the quarantine is performed by the firewall client. **Freund** in an analogous art discloses a client-based filter application *(firewall)* for monitoring whether client process has access to the Internet otherwise the remediation for any violated rule is performed (see column 4, lines 29-33 and lines 54-63); and further discloses limiting the user access to the network in case of any problems including malfunction, tampering,with remediating the network (see column 22, lines 30-41); **Freund** discloses in a preferred embodiment all the filtering process may be performed by the client-based filter application *(firewall)* (see column 4, lines 29-33). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to perform the quarantine *by a firewall residing on said computer system.* One of ordinary skill in the art would have recognized some of advantages suggested by **Freund** for having the user firewall performing some of the filtering work; the advantages of doing so would reduce the workload of the server and would avoid a centralized filtering mechanism misinterpreting the rules to apply to data packets as suggested by **Freund** (see column 2, lines 38-46 and 59-63).

As per claim 16, the references as combined above disclose the network security scanning the client that meets the recitation of *wherein said nefarious software detection and removal is performed by said computer network* (see **Shaw,** paragraph 38). Claim 16 is also rejected on the same rationale as claim 14 for the disclosure of software removal.

As per claim 17, the references as combined above disclose the virus scanner for performing the scanning of viruses that meets the recitation of *wherein said nefarious software detection and removal is performed by said computer system* (see **Shaw,** paragraph 38).

As per claim 18, the references as combined above disclose restricting access to certain approved applications (see **Freund,** column 8, lines 45-47). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to restrict access to *traffic related to said nefarious software detection and removal* so as to meet the security requirements to gain access to the network as suggested by **Shaw** (see par. 39).

As per claims 19-20, the references as combined above disclose *wherein said nefarious software is a computer virus* and discloses *wherein said nefarious software is a worm* (see **Shaw** par. 17).

4.4 **Claims 27-28 and 30-31** are rejected under 35 U.S.C. 103(a) as being unpatentable by US Patent Publication 2005/0188419 to **Dadhia et al.**

As per claims 27-28, **Dadhia et al** substantially discloses the claimed network of claim 22 and further discloses the *computer system is configured to raise said firewall upon initiating registration with a LAN* (see paragraph 18). **Dadhia et al** discloses that the invention is not limited with some of the exemplary networks mentioned (see paragraphs 20-21). **Dadhia et al** is silent about using a virtual private network which is well known in the art of computer network security. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement the invention of **Dadhia et al** with any type of network as known in the art because using a VPN or WVPN network does not functionally relate to the to the steps in the network claimed and because it does not patentably distinguish the claimed invention.

As per claim 30, **Dadhia et al** substantially discloses *a computer system, comprising:* processor, memory, that meets the recitation of *a processor subsystem; a memory subsystem coupled to said processor subsystem* (see paragraph 20)*; at least one application* (instance of an application or operating system) *residing in said memory subsystem and executable by said processor subsystem* (see paragraph 18); *and a firewall switchable between a closed position in which traffic to and/or from said computer system is restricted and an open position in which traffic to and/or from said computer system is unrestricted* (see paragraph 18)*; wherein said firewall is configured to switch into said closed position upon power-up of said computer system and upon initiation of registration with a computer network* (see page 4, claim 2). As interpreted by the Examiner a firewall can be active/inactive or enabled/disabled, or turned on/off that meets the recitation of switchable firewall with closed/open position as claimed. **Dadhia et al** discloses that the firewall may be configured to restrict access to only resources that will allow it to update (see par. 25) and the dynamic protection system applies filtering rules to the application upon startup (*upon power-up)* and access (*upon initiation of registration)* to the network. Although not using the same terms, **Dadhia et al** disclosure reads into the claimed invention and it would have been obvious to one of ordinary skill in the art at the time the invention was made to configure the firewall to limit access to resources (page 2, lines 1-7) upon startup (*upon power-up)* of the computer system and access (*upon initiation of registration)* to the network (see page 4, claim 2) because it would ensure that the application is up-to-date as soon as the application is started and a vulnerability is not exploited as suggested by **Dadhia et al** (see page 2, paragraph 14).

As per claim 31, **Dadhia et al** discloses that the firewall may be configured to restrict access only to resources that will allow it to update the patches *(remediation)* (see par. 25 and paragraph 12) that meets the recitation of *wherein said firewall is configured to pass, in said closed position, first and second types of traffic, said first type of traffic being related to registration of said computer system with said computer network and said second type of traffic being related to remediation of said computer system by a client remediation server coupled to said computer network.*

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses many of the claimed features such as isolating a computer system until remediation is performed. (See form 892).

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin
Patent Examiner
December 8, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

12, 8, 06